Methods and apparatus for a computer network firewall with multiple domain support

Patent Number: EP0909074

Publication date: 1999-04-14

Inventor(s): COSS MICHAEL JOHN (US); MAJETTE DAVID L (US); SHARP RONALD L

Applicant(s): LUCENT TECHNOLOGIES INC (US)

Requested Patent: JP11168511

Application EP19980306998 19980901

Priority Number(s): US19970927382 19970912

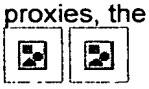
IPC Classification: H04L29/06

EC Classification: H04L29/06, H04L29/06C6A

Equivalents:

Abstract

The invention provides improved computer network firewalls which include one or more features for increased processing efficiency. A firewall in accordance with the invention can support multiple security policies, multiple users or both, by applying any one of several distinct sets of access rules. The firewall can also be configured to utilize "stateful" packet filtering which involves caching rule processing results for one or more packets, and then utilizing the cached results to bypass rule processing for subsequent similar packets. To facilitate passage to a user, by a firewall, of a separate later transmission which is properly in response to an original transmission, a dependency mask can be set based on session data items such as source host address, destination host address, and type of service. The mask can be used to query a cache of active sessions being processed by the firewall, such that a rule can be selected based on the number of sessions that satisfy the query. Dynamic rules may be used in addition to pre-loaded access rules in order to simplify rule processing. To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－168511

(43)公開日　平成11年(1999)６月22日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　12/66		Ｈ０４Ｌ　11/20	Ｂ
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ｚ
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｅ
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｂ
			６７３Ａ

審査請求　未請求　請求項の数26　ＯＬ　（全 18 頁）

(21)出願番号　特願平10－252832

(22)出願日　平成10年(1998)９月７日

(31)優先権主張番号　０８／９２７３８２

(32)優先日　1997年９月12日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　596077259
ルーセント　テクノロジーズ　インコーポレイテッド
Ｌｕｃｅｎｔ　Ｔｅｃｈｎｏｌｏｇｉｅｓ　Ｉｎｃ．
アメリカ合衆国　07974　ニュージャージー、マレーヒル、マウンテン　アベニュー　600－700

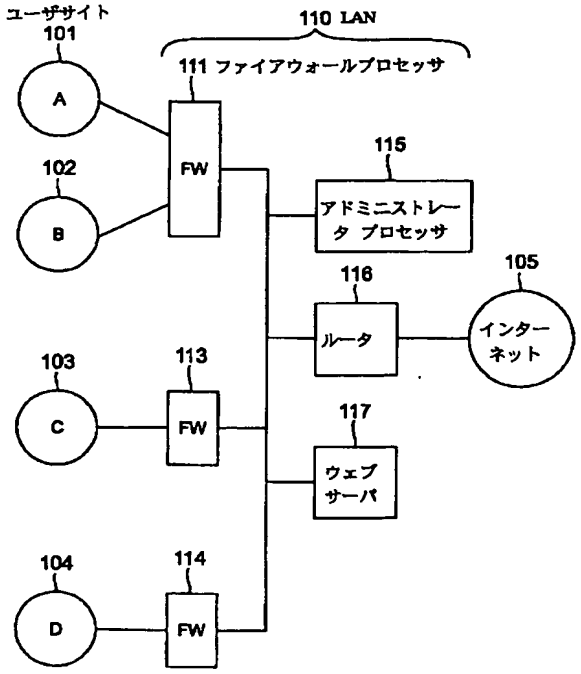
(72)発明者　マイケル　ジョン　コス
アメリカ合衆国，08807　ニュージャージー，ブリッジウォーター，ウェックスフォード　ウェイ　28

(74)代理人　弁理士　三俣　弘文

最終頁に続く

(54)【発明の名称】　パケット検証方法

(57)【要約】
【課題】　単一のファイアウォールが、それぞれ別々のセキュリティポリシーを有する複数のユーザをサポートすることを可能にする。
【解決手段】　ファイアウォールは、パケットに対するセッションキーを導出し、セッションキーに基づいて複数のセキュリティポリシーのうちから少なくとも１つのセキュリティポリシーを選択し、選択されたセキュリティポリシーを用いてパケットを検証する。実施例では、セッションキーはパケットのヘッダ情報から導出される項目を含む。この項目としては、例えば、ＩＰソース／デスティネーションアドレス、次のレベルのプロトコル、該プロトコルに関係づけられたソース／デスティネーションポートがある。また、次のレベルのプロトコルは、例えば、ＴＣＰまたはＵＤＰである。セキュリティポリシーは、相異なるグループ、あるいは、与えられたグループ内の相異なるサブグループに対応する。



【特許請求の範囲】
【請求項１】　コンピュータネットワークにおけるパケットを検証する方法において、該方法は、
前記パケットに対するセッションキーを導出するステップと、
前記セッションキーの関数として複数のセキュリティポリシーのうちから少なくとも１つのセキュリティポリシーを選択する選択ステップと、
選択されたセキュリティポリシーを用いて前記パケットを検証するステップとからなることを特徴とするパケット検証方法。
【請求項２】　前記セッションキーは、前記パケット内のデータに付加されるヘッダ情報から導出される項目を含むことを特徴とする請求項１に記載の方法。
【請求項３】　前記セッションキーは、
（ｉ）ソースアドレス、
（ｉｉ）デスティネーションアドレス、
（ｉｉｉ）次のレベルのプロトコル、
（ｉｖ）プロトコルに関係づけられたソースポート、および
（ｖ）該プロトコルに関係づけられたデスティネーションポート、
からなるセットからの少なくとも１つの項目を含むことを特徴とする請求項１に記載の方法。
【請求項４】　前記セッションキーは、
（ｉ）インターネットプロトコル（以下「ＩＰ」という。）ソースアドレス、
（ｉｉ）ＩＰデスティネーションアドレス、
（ｉｉｉ）次のレベルのプロトコル、
（ｉｖ）該プロトコルに関係づけられたソースポート、および
（ｖ）該プロトコルに関係づけられたデスティネーションポート、
からなるセットからの少なくとも１つの項目を含むことを特徴とする請求項１に記載の方法。
【請求項５】　前記次のレベルのプロトコルは、伝送制御プロトコルＴＣＰまたはユーザデータグラムプロトコルＵＤＰであることを特徴とする請求項３に記載の方法。
【請求項６】　前記ネットワークは複数のネットワークインタフェースを含み、
前記選択ステップは、要求が受信されたインタフェースを判定するステップを含むことを特徴とする請求項１に記載の方法。
【請求項７】　前記ネットワークは複数のネットワークインタフェースを含み、
前記選択ステップは、要求の送信先のインタフェースを判定するステップを含むことを特徴とする請求項１に記載の方法。
【請求項８】　コンピュータネットワークにおけるパケットを検証する方法において、該方法は、
それぞれアクセスルールのセットを含む複数の独立のセキュリティポリシーを指定するステップと、
前記パケットにはいずれのセキュリティポリシーが適当であるかを判定するステップと、
判定されたセキュリティポリシーのアクセスルールのセットを用いて前記パケットを検証するステップとからなることを特徴とするパケット検証方法。
【請求項９】　複数のセキュリティポリシーの少なくとも一部は、単一のファイアウォールに関連づけられた相異なるグループに対応することを特徴とする請求項８に記載の方法。
【請求項１０】　複数のセキュリティポリシーの少なくとも一部は、与えられたグループ内の相異なるサブグループに対応することを特徴とする請求項８に記載の方法。
【請求項１１】　与えられたグループのアドミニストレータのみが、該グループのセキュリティポリシーのルールを修正する権限を有することを特徴とする請求項８に記載の方法。
【請求項１２】　コンピュータネットワークのファイアウォールでパケットを検証する際に用いられる装置において、
前記ファイアウォールは複数の独立のセキュリティポリシーを指定し、各セキュリティポリシーはアクセスルールのセットを含み、
前記装置は、
前記ファイアウォールにおいて、（ｉ）前記パケットにはいずれのセキュリティポリシーが適当であるかを判定し、（ｉｉ）判定されたセキュリティポリシーのアクセスルールのセットを用いて前記パケットを検証する、プロセッサを有することを特徴とする、パケットを検証する際に用いられる装置。
【請求項１３】　複数のセキュリティポリシーの少なくとも一部は、単一のファイアウォールに関連づけられた相異なるグループに対応することを特徴とする請求項１２に記載の装置。
【請求項１４】　複数のセキュリティポリシーの少なくとも一部は、与えられたグループ内の相異なるサブグループに対応することを特徴とする請求項１２に記載の装置。
【請求項１５】　与えられたグループのアドミニストレータのみが、該グループのセキュリティポリシーのルールを修正する権限を有することを特徴とする請求項１２に記載の装置。
【請求項１６】　コンピュータネットワークにおけるファイアウォールを提供する方法において、該方法は、
アクセスルールを複数のドメインに分割するステップと、
与えられたドメインのアドミニストレータのみが該ドメ

インのセキュリティポリシーのルールを修正する権限を有するように前記アクセスルールを管理するステップとからなることを特徴とする、ファイアウォールを提供する方法。

【請求項１７】　コンピュータネットワークにおけるパケット検証を行うコンピュータシステムにおいて、該コンピュータシステムは、

セッションを求める要求から少なくとも１つのデータ項目を取得する手段と、

前記データ項目の関数として複数のセキュリティポリシーのうちから少なくとも１つのセキュリティポリシーを選択する選択手段と、

選択されたセキュリティポリシーを用いて前記セッションのパケットを検証する手段とからなることを特徴とするコンピュータシステム。

【請求項１８】　前記ネットワークは複数のネットワークインタフェースを含み、

前記選択手段は、要求が受信されたインタフェースを判定する判定手段を含むことを特徴とする請求項１７に記載のコンピュータシステム。

【請求項１９】　前記判定手段は、前記要求に含まれるソースＩＰアドレスを参照する手段を含むことを特徴とする請求項１８に記載のコンピュータシステム。

【請求項２０】　前記ネットワークは複数のネットワークインタフェースを含み、

前記選択手段は、要求の送信先のインタフェースを判定する判定手段を含むことを特徴とする請求項１７に記載のコンピュータシステム。

【請求項２１】　前記判定手段は、前記要求に含まれるデスティネーションＩＰアドレスを参照する手段を含むことを特徴とする請求項２０に記載のコンピュータシステム。

【請求項２２】　コンピュータネットワークにおけるパケット検証方法において、該方法は、

セッションを求める要求から少なくとも１つのデータ項目を取得するステップと、

前記データ項目の関数として複数のセキュリティポリシーのうちから少なくとも１つのセキュリティポリシーを選択する選択ステップと、

選択されたセキュリティポリシーを用いて前記セッションのパケットを検証するステップとからなることを特徴とするパケット検証方法。

【請求項２３】　前記ネットワークは複数のネットワークインタフェースを含み、

前記選択ステップは、要求が受信されたインタフェースを判定する判定ステップを含むことを特徴とする請求項２２に記載の方法。

【請求項２４】　前記判定ステップは、前記要求に含まれるソースＩＰアドレスを参照するステップを含むことを特徴とする請求項２３に記載の方法。

【請求項２５】　前記ネットワークは複数のネットワークインタフェースを含み、

前記選択ステップは、要求の送信先のインタフェースを判定する判定ステップを含むことを特徴とする請求項２２に記載の方法。

【請求項２６】　前記判定ステップは、前記要求に含まれるデスティネーションＩＰアドレスを参照するステップを含むことを特徴とする請求項２５に記載の方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンピュータネットワークにおける権限のないアクセスの防止に関し、特に、コンピュータネットワーク内のファイアウォール保護に関する。

【０００２】

【従来の技術】コンピュータネットワークでは、情報は、通常、パケットの形で伝送される。あるサイトにある情報は、そのサイトまたは別のサイトのコマンドで、別のサイトからアクセスされ、あるいは、別のサイトへ送信される。従って、例えば情報が財産である場合、権限のないアクセスに対する保護の必要がある。このために、ファイアウォールとして知られるワークプロセッサコンポーネントで実行される、パケットフィルタリングという技術が開発され市販されている。ファイアウォールでは、パケットは検査されフィルタリングされる。すなわち、あらかじめ定義されたアクセスルールのセットに従っているかどうかに応じて、パケットは、通過し、あるいは、廃棄される。通常、このルールセットは表形式で表される。

【０００３】一般に、ファイアウォールアドミニストレータは、ファイアウォールの一方の側から他方の側へは、同意された広範なアクセスを許容するが、アクティブなネットワークセッションの一部ではない逆向きの伝送は遮断する。例えば、会社の「内部」の従業員はファイアウォールを通じてインターネットのような「外部」のネットワークに無制限にアクセスすることができるが、インターネットからのアクセスは、特別に権限を与えられていなければ遮断される。このような、会社とインターネットの境界にあるファイアウォールに加えて、ファイアウォールは、ネットワークドメイン間にも置かれることがあり、また、ドメイン内でも、サブドメインを保護するために用いられることがある。それぞれの場合において、異なるセキュリティポリシーが関係している。

【０００４】いくつかの複雑なネットワークプロトコルでは、外部からユーザへ戻る別個の追加のネットワークセッションが必要とされる。そのような複雑なプロトコルの１つは、RealAudioという商品名で知られているサービスによって用いられている。特別の処置がなければ、この別個のセッションに対する要求はファイアウォ

ールによって遮断されてしまう。
【０００５】このような複雑なプロトコルに対して、ユーザの代わりにファイアウォールプロセッサ上で並行して走る別個の「プロキシ」プロセスが開発されている。プロキシプロセスは、別の特殊目的アプリケーション、例えば、認証、メール処理、およびウィルススキャンのようなサービスを実行するためにも、開発されている。
【０００６】
【発明が解決しようとする課題】ファイアウォールプロセッサが並行プロセスをサポートする容量には限界があるので、並行して走らせることができるセッションの数を最大にするためには、ファイアウォール上のプロキシプロセスに対する需要を最小にすることが好ましい。さらに、このような最小化は、全伝送レートに関しても、好ましい。その理由は、入力データが別々のプロセスを通ると伝送が遅くなるためである。
【０００７】
【課題を解決するための手段】本発明は、処理効率を改善し、セキュリティを改善し、アクセスルール自由度を増大させ、複雑なプロトコルを扱うファイアウォールの能力を高めるように、コンピュータネットワークのファイアウォールを実現する技術を提供する。本発明の第１の特徴によれば、コンピュータネットワークファイアウォールは、与えられたパケットに対していくつかの別個のアクセスルールセットのうちのいずれかを適用することによって、（ａ）複数のセキュリティポリシー、（ｂ）複数のユーザ、または、（ｃ）複数のセキュリティポリシーおよび複数のユーザの両方をサポートすることができる。パケットに対して適用されるルールセットは、入出力ネットワークインタフェースや、ネットワークのソースおよびデスティネーションのアドレスのような情報に基づいて決定される。
【０００８】本発明の第２の特徴によれば、コンピュータネットワークファイアウォールは、パケットに適用されるルール処理の結果を記憶することによって性能を改善する「状態付き」パケットフィルタリングを利用するように構成される。状態付きパケットフィルタリングは、パケットに対するルール処理結果をキャッシュし、キャッシュされた結果を利用して後続の同種のパケットに対するルール処理を迂回することによって実現される。例えば、あるネットワークセッションの特定のパケットにルールセットを適用した結果をキャッシュし、同じネットワークセッションからの後続のパケットがファイアウォールに到着したときに、キャッシュされている前のパケットからの結果を、その後続パケットに対して用いる。これにより、それぞれの入力パケットにそのルールセットを適用する必要がなくなる。
【０００９】本発明の第３の特徴によれば、コンピュータネットワークファイアウォールは、ソースホストアドレス、デスティネーションホストアドレス、およびサービスタイプのようなセッションデータ項目に基づいて設定することが可能な依存関係マスクを用いて、ネットワークセッションを認証あるいは阻止する。依存関係マスクを用いて、ファイアウォールによって処理されているアクティブセッションのキャッシュに問合せをすることが可能であり、それにより、問合せを満たすセッションの数を識別することができる。この問合せを、アクセスルールに対応させ、特定のルールのセッションが、その問合せに適合する数に依存するようにすることが可能である。
【００１０】本発明の第４の特徴によれば、コンピュータネットワークファイアウォールは、パケットを処理するためのアクセスルールのセットに追加された動的ルールを利用することが可能である。動的ルールによれば、与えられたルールセットは、ルールセット全体をリロードすることを要求せずに、ネットワークにおいて起こるイベントに基づいて修正される。動的ルールの例としては、単一のセッションに対してのみ用いられる「ワンタイム」ルール、指定された期間に対してのみ用いられる時限ルール、および、ある条件が満たされたときにのみ用いられるしきい値ルールがある。他のタイプの動的ルールとしては、ホストグループを定義するルールがある。この動的ルールによれば、アクセスルールセットの他の事項を変更せずに、ホストを追加あるいは削除するようにホストグループを変更することができる。
【００１１】本発明の第５の特徴によれば、アプリケーションプロキシのファイアウォールの負担を軽減するように、処理のための別のサーバにネットワークセッションをリダイレクトするようコンピュータネットワークファイアウォールに対して指令することができる。この別サーバは、リダイレクトされたネットワークセッションを処理した後、そのセッションを、ファイアウォールを通じて、もとの意図されたデスティネーションへ渡す。
【００１２】本発明のコンピュータネットワークファイアウォールにより、広範囲の重要なアプリケーションでのファイアウォール処理が可能となる。例えば、本発明は、ダイヤルアップアクセスゲートウェイに実装可能である。本発明の別の実施例では、ファイアウォールの第１部分がネットワークに存在し、ファイアウォールの第２部分がセットトップボックス、コンピュータあるいはその他の、家庭または会社にあるユーザ端末にあるというように分散的にも実装可能である。後者の実施例によれば、本発明のファイアウォール技術は、例えば、家庭においてインターネットとビデオアクセスの親による制御を提供することが可能である。
【００１３】
【発明の実施の形態】ファイアウォールにおいて、例えば、別個のローカルエリアネットワーク（ＬＡＮ）間あるいはＬＡＮのサブネット間でのデータの流れを制御する好ましい技術が実現される。以下で、本発明の実施例

は、プロセスに関して説明する。このようなプロセスの効率的なプロトタイプは、汎用ＰＣハードウェア上に実装するためにプログラミング言語Ｃを用いて、コンピュータシステムソフトウェアとして実現されている。専用のファームウェアあるいはハードウェアのコンピュータシステム実装により、さらに効率を向上させることも可能である。

【００１４】１．複数のセキュリティドメインのサポート

複数のセキュリティドメインをサポートする能力により、単一のファイアウォールが、それぞれ別々のセキュリティポリシーを有する複数のユーザをサポートすることが可能となる。また、相異なるセキュリティポリシーをサブサイト間の通信に適用することができるため、このような能力は、サイト内でも使用可能である。それぞれの構成を図１および図２に例示する。

【００１５】図１に、インターネット１０５への接続にファイアウォールを有する４つのユーザサイト１０１～１０４（例として、会社Ａ～Ｄ）を示す。このような保護は、ファイアウォール設備によって提供される。ファイアウォール設備は、ここではＬＡＮ１１０の形態であり、ファイアウォールプロセッサ１１１、１１３および１１４、アドミニストレータプロセッサ１１５、ルータ１１６ならびにウェブサーバ１１７を有する。ファイアウォールプロセッサ１１３および１１４はそれぞれ単一のサイト（すなわち、それぞれサイト１０３および１０４）専用である。ファイアウォールプロセッサ１１１は、２つのサイト１０１および１０２にサービスするように設定される。ファイアウォールプロセッサ１１１は、２つのサイトそれぞれとインターネット１０５との間、および、２つのサイト間の通信に、別々のファイアウォールポリシーを実装する。ファイアウォールプロセッサ１１１の好ましい動作のためのプロセスについて、複数のファイアウォールポリシーのうちからの適切な選択を含めて、図５および図６を参照して後述する。

【００１６】図２に、ファイアウォールプロセッサ２１１を通じてインターネット１０５に接続されたユーザサイト２０１を示す。アドミニストレータプロセッサ２１５およびルータ２１６は、ファイアウォールプロセッサ２１１に接続される。ルータ２１６は、ユーザサイト２０１の内部にある別のファイアウォールプロセッサ２１２および２１３に接続される。ファイアウォールプロセッサ２１２は、単一のサブサイト２２３（例として人事（ＨＲ））を保護する。ファイアウォール２１３は、２つのサブサイト（例として、給与（Ｐ）および支払（Ｄ））を、サイト２０１の残りの部分に対して、および、サブサイト２２１と２２２の間の通信に関して、保護するように設定される。これは、ファイアウォールプロセッサ２１３において、図５および図６で例示されるプロセスを用いることによって達成される。

【００１７】セキュリティポリシーは、アクセスルールのセットによって表現される。アクセスルールのセットは、表（テーブル）形式で表され、ファイアウォールアドミニストレータによってファイアウォールにロードされる。図３に示すように、このようなテーブルは、ルール番号、ソースおよびデスティネーションのホストの名称、パケットで要求されることが可能な特殊サービスの名称、および、パケットに対してなされるアクションの指定を含むカテゴリに対して与えられる。特殊サービスには、例えば、プロキシサービス、ネットワークアドレス翻訳、および、暗号化が含まれる。図３では、「ソースホスト」、「デスティネーションホスト」および「サービス」というカテゴリは、パケットに対して指定されたアクションがなされるために、そのパケットに含まれるデータが満たさなければならない条件を課している。他の条件を含めることも可能であり、そのような条件は、必ずしも、パケットに含まれるデータに関係する必要はない。例えば、ルールの適用は、日時に関して条件づけられることも可能である。

【００１８】あるルールにおいて、ルールテーブルに与えられたカテゴリが無関係である場合、対応するテーブルエントリは「ワイルドカード」とマークされる。これは、任意のカテゴリあるいはカテゴリの組合せに適用可能である。図３などでは、ワイルドカードエントリにアステリスク（＊）を用いている。「ＦＴＰ」はファイル転送プロトコル(file transfer protocol)を表す。

【００１９】パケットに対するルール処理において、パケットによって満たされるルールが見つかるまで（または、ルールテーブルの最後まで。その場合、そのパケットは廃棄される。）、ルールは順に適用される。ルールを満たすパケットに対して、そのルールに含まれる各条件が満たされなければならない。例えば、図３において、ソースホストＡからデスティネーションホストＤへの、メールを表すパケットは、ルール２０により廃棄される。以下は、本発明による例示的なルールセットカテゴリのさらに詳細なリストである。最初の５個のカテゴリ名は、図３のカテゴリに対応する。

【００２０】カテゴリ名：ルール番号

説明：ドメイン内のルールの番号。ルール番号は、一意的である必要はないが、一般に、単一のサービス（例えばＦＴＰ）を表すべきである。

【００２１】カテゴリ名：ソースホスト

説明：ソースホストグループの識別子またはＩＰアドレス。

【００２２】カテゴリ名：デスティネーションホスト

説明：デスティネーションホストグループの識別子またはＩＰアドレス。

【００２３】カテゴリ名：サービス

説明：サービスのグループまたはプロトコル／デスティネーションポート／ソースポート。

【００２４】カテゴリ名：アクション
説明：ルールアクション、例えば、「通過」、「廃棄」または「プロキシ」。
【００２５】カテゴリ名：廃棄通知
説明：ＹＥＳの場合、アクションが「廃棄」であれば、インターネット制御メッセージプロトコル（ＩＣＭＰ）メッセージが送出される。
【００２６】カテゴリ名：キャッシュタイムアウト
説明：セッションエントリがキャッシュから除去されるまでのアクティビティなしの秒数。
【００２７】カテゴリ名：リセットセッション
説明：ＹＥＳの場合、ＴＣＰセッションに対して、キャッシュタイムアウト時にコネクションの両端にＴＣＰリセットを送る。
【００２８】カテゴリ名：ルールタイムアウト
説明：ルールがルールリストから除去されるまでのアクティビティなしの秒数。
【００２９】カテゴリ名：開始期間
説明：ルールに対する開始アクティブ期間。
【００３０】カテゴリ名：終了期間
説明：ルールに対する終了アクティブ期間。
【００３１】カテゴリ名：期間終了時セッション消去
説明：ＹＥＳの場合、このルールによって許可されたセッションは期間終了時に消去(kill)される。
【００３２】カテゴリ名：依存関係マスク
説明：依存関係マスク名。
【００３３】カテゴリ名：入力インタフェース
説明：受信時に一致すべきインタフェース名。
【００３４】カテゴリ名：出力インタフェース
説明：パケットが送信されるインタフェース名。
【００３５】カテゴリ名：監査セッション
説明：監査記録生成。ＹＥＳの場合、セッションの開始時および終了時に監査記録が生成される。
【００３６】カテゴリ名：アラームコード
説明：ルールを特定のアラームに結び付けるために用いられるアラームコード値。
【００３７】カテゴリ名：ソースホストマップグループ
説明：ＩＰアドレス、または、マップ先のホストＩＰアドレスを含むホストグループ。
【００３８】カテゴリ名：ソースホストマップタイプ
説明：実行されるマッピングのタイプ（例えば、「プール」あるいは「直接」）。
【００３９】カテゴリ名：デスティネーションホストマップグループ
説明：ＩＰアドレス、または、マップ先のホストＩＰアドレスを含むホストグループ。
【００４０】カテゴリ名：デスティネーションホストマップタイプ
説明：実行されるマッピングのタイプ（例えば、「プール」あるいは「直接」）。
【００４１】カテゴリ名：サービスマップグループ
説明：マップ先のデスティネーションポート番号またはデスティネーションポートを含むサービスグループ。参照されるサービスグループ内のプロトコルおよびソースポートは無視される。
【００４２】カテゴリ名：サービスマップタイプ
説明：実行されるマッピングのタイプ（例えば、「プール」あるいは「直接」）。
【００４３】カテゴリ名：最大使用総数
説明：このルールが使用されることが可能な最大回数。この限界に達するとルールは除去される。
【００４４】カテゴリ名：最大使用並行数
説明：与えられた時刻にアクティブであることが可能な、このルールによって許可されるセッションの最大数。この数が、指定された値を下回るまで、ルールはイナクティブである。
【００４５】カテゴリ名：コピー先アドレス
説明：パケットのコピーが送られるアプリケーションのアドレス。セッションキャプチャに用いられる。
【００４６】カテゴリ名：トンネルデスティネーション
説明：トンネルを設定し、それをこのデスティネーションアドレスおよびプロトコルに送る。新しいＩＰヘッダがパケットに追加される。
【００４７】カテゴリ名：トンネル条件
説明：トンネリングが必要となるときを示す。ＮＵＬＬの場合、チェックは不要である。ＩＮの場合、入力セッションはトンネリングされていなければならない。ＯＵＴの場合、パケットをトンネリングするアクションを開始する。ＢＯＴＨの場合、両方を行う。
【００４８】カテゴリ名：ＩＰＳＥＣ条件
説明：ＩＰセキュリティ（ＩＰＳＥＣ(IP Security)）処理が必要となるときを示す。ＮＵＬＬの場合、チェックは不要である。ＩＮの場合、入力セッションはＩＰＳＥＣを用いて保護されていなければならない。ＯＵＴの場合、ＩＰＳＥＣ保護を追加するアクションを開始する。ＢＯＴＨの場合、両方を行う。
【００４９】カテゴリ名：シーケンス番号ランダム化
説明：ＴＣＰシーケンス番号をランダム化するオプション。デフォルトはＮＯである。
【００５０】カテゴリ名：Syn Storm保護
説明：Syn Storm攻撃からの保護を提供する。デフォルトはＮＯである。
【００５１】カテゴリ名：復帰チャネル許可
説明：ＹＥＳの場合、初期パケットは同じアクションでキャッシュに順チャネルおよび逆チャネルを生成する。デフォルトはＹＥＳである。
【００５２】２．状態付きパケットフィルタリング
本発明によるコンピュータネットワークファイアウォールは、「状態付き」パケットフィルタリングを利用するように設定することができる。状態付きパケットフィル

タリングは、パケットに適用されたルール処理の結果をキャッシュに記憶することによって性能を改善する。状態付きパケットフィルタリングは、受信パケットに対するルール処理結果をキャッシュし、その後、キャッシュされた結果を利用して、同様のパケットに対するルール処理を迂回することにより実現される。例えば、与えられたネットワークセッションのパケットにルールセットを適用した結果をキャッシュし、同じネットワークセッションからの後続のパケットがファイアウォールに到着したときに、前のパケットからのキャッシュされた結果をその後続パケットに対して使用するようにする。これによって、入力パケットのそれぞれにルールセットを適用する必要がなくなることにより、従来のファイアウォールに比べて大幅な性能向上が実現する。

【００５３】キャッシュエントリの数はルールの数の何倍にもなり得るため、キャッシュの効率的使用は、（例えばハッシュテーブルを用いた）索引付けを必要とすることがある。図４に示すように、キャッシュは「セッションキー」、ハードウェアアドレス情報、インタフェース情報、適用可能なルールの数、アラームコード、統計情報、および適用可能なアクションを含むことが可能である。セッションキーは、パケット内で送信されるデータに付加された少なくとも１つのヘッダ項目を含み、実施例では、（ｉ）インターネットプロトコル（ＩＰ）ソースアドレス、（ｉｉ）ＩＰデスティネーションアドレス、（ｉｉｉ）次のレベルのプロトコル（例えば、伝送制御プロトコル（ＴＣＰ）またはユーザデータグラムプロトコル（ＵＤＰ））、（ｉｖ）プロトコルに関連づけられたソースポート、および（ｖ）プロトコルに関連づけられたデスティネーションポート、を含む。図４では、セッションキーに対して、項目（ｉ）および（ｉｉ）は個別に示されている。項目（ｉｉｉ）～（ｖ）は、略して「ＴＥＬＮＥＴ」および「ＭＡＩＬ」で表されている。

【００５４】ファイアウォールでは、ここで「ドメインサポートエンジン（ＤＳＥ(domainsupport engine)）と呼ぶ判断モジュール（エンジン）が、新しいネットワークセッションに対していずれのセキュリティポリシーを使用すべきかを判断する。新しいセッションはそれぞれ、ソースドメインおよびデスティネーションドメインのセキュリティポリシーによって承認されなければならない。インターネットへ向かうコネクションでは、単一のドメインの検査のみが実行される可能性が高い。ＤＳＥは、入力または出力ネットワークインタフェースと、各パケットのソースまたはデスティネーションネットワークアドレスに基づいて、ドメイン選択を行う。ソースまたはデスティネーションのアドレスをパケットに含めることにより、複数のユーザが、単一のネットワークインタフェースによってサポートされることが可能となる。入力または出力ネットワークインタフェースは、ネットワークインタフェースカード（ＮＩＣ）（例えばインテル社(Intel Corporation)から市販されているIntel EtherExpress Pro 100Bカード）の形態のものが可能である。

【００５５】図５および図６は、複数のドメインをサポートするファイアウォールによるパケット処理の全体流れ図である。このような処理は、パケットが行くドメインを判断し、適用可能なルールを検査してパケットが通ってもよいかどうかを確認し、特殊処理が必要稼働かを判断することを含む。ファイアウォールでは、各ドメインには１つ以上のネットワークインタフェースが関係づけられる。複数のドメインをサポートするインタフェースは、ＩＰアドレスレンジを用いて、パケットを区別するように分離される。以下のステップが含まれる。

【００５６】５０１：ＩＰパケットがインタフェースでファイアウォールにより受信される。

【００５７】５０２：パケットのＩＰヘッダからセッションキーが取得される。

【００５８】５０３：いずれのインタフェースがパケットを受信したか、および、受信パケットのソースＩＰアドレスに基づいて、ソースドメインが、図７および図８に関して別に後述するように判定される。ドメインが見つからない場合、プロセスはステップ５０５に飛ぶ。

【００５９】５０４：ステップ５０２からのセッションキーを用いて、ソースドメインのキャッシュでの一致を探索する。キャッシュ内に一致があり、アクションが「廃棄」の場合、パケットは廃棄され、プロセスはステップ５０１に戻る。キャッシュ内に一致がない場合、ソースドメインのルールセットで一致を探索する。ルールで一致があり、アクションが「廃棄」でない場合、プロセスはステップ５０５に進む。ルールで一致があり、アクションが「廃棄」の場合、対応するエントリがキャッシュに含められ、パケットは廃棄され、プロセスはステップ５０１に戻る。ルールで一致がない場合、パケットは廃棄され、プロセスはステップ５０１に戻る。

【００６０】５０５：パケットのローカルエリアネットワーク（ＬＡＮ）アドレスを用いて、しかも、ソースドメインルールがデスティネーションインタフェースを指定している場合には、そのデスティネーションインタフェースおよびルーティングテーブルを用いて、デスティネーションインタフェースが決定される。

【００６１】５０６：デスティネーションインタフェースおよびパケットのデスティネーションアドレスを用いて、デスティネーションドメインが決定される。デスティネーションドメインが見つからない場合、または、デスティネーションドメインが直前に検査したドメインと一致する場合、プロセスはステップ５０８に進む。

【００６２】５０７：ソースドメインに関してステップ５０４で用いられるのと同様にして、デスティネーションドメインに関して、キャッシュルックアップと、必要

であればルールセットルックアップを行う。
【００６３】５０８：パケットに適用されるルールがアドレス変更（例えば、プロキシへの）を要求する場合、あるいは、あるパケットを別のパケット内に挿入すること（「トンネルオプション」）を要求する場合、プロセスは、変更されたデスティネーションに基づく処理のためにステップ５０５に戻る。
【００６４】５０９：パケットがいずれのドメインに関しても処理されなかった場合、ファイアウォール所有者はいずれのアクセスルールにも従わないインタフェース間の通信をサポートすることには関心がないので、そのパケットは廃棄可能である。
【００６５】５１０：すべてのアクションの結果が「通過」であった場合、パケットは適当なネットワークインタフェースへ送出される。
【００６６】各ネットワークインタフェースからドメインへの簡便なリンクのために、ドメインテーブルが用いられる。インタフェースが複数のドメインによって共有されている場合、アドレスレンジが含められる。これは図７に例示されている。図７には、重複のないアドレスレンジが示されている。
【００６７】図８に、上記のステップ５０３および５０６で実行されるようなドメインテーブル処理を例示する。これには以下のステップが含まれる。
【００６８】７０１：ドメインテーブルでインタフェース名が一致するものを探索する。
【００６９】７０２：一致するテーブルエントリが見つかった場合、しかも、ＩＰアドレスレンジが一致するテーブルエントリにある場合、パケットアドレスがそのレンジ内にあるかどうかを検査する。レンジ内にある場合、指定されたドメインが選択される。レンジ内にない場合、次のテーブルから探索を継続する。
【００７０】７０３：一致するものがないままテーブルの終端に到達した場合、何のアクションもとらない。
【００７１】３．依存関係マスク
例えばRealAudioによって用いられるプロトコルのような、外部からユーザに戻る別個の追加のネットワークセッションを要求するタイプのプロトコルの場合、ルールは、ユーザに戻るコネクションを許可する条件あるいはマスクを含むことが可能である。ただしそれは、並行してアクティブである正当な順方向のコネクション（すなわち、ソースとデスティネーションのアドレスを入れ替えたコネクション）がある場合に限る。その結果、ファイアウォール上に別個のあるいはプロキシのアプリケーションが不要となる。
【００７２】本発明による依存関係マスクは、セッションキャッシュに向けられた問合せを定義することができる。マスクで定義されるすべてのフィールドを、キャッシュ内の対応するフィールドと比較することによって、一致の有無が判定される。マスク内の空フィールドは比較に用いられない。
【００７３】依存関係マスクは、（ａ）パケット内の情報、（ｂ）そのパケットのソースインタフェース、および（ｃ）そのパケットが通過するために満たさなければならない１つまたはいくつかの依存条件、を用いて、ネットワークセッションの最初のパケットに対するルールで定義することが可能である。このような最初のパケットがファイアウォールによって処理されると、対応するエントリがキャッシュに作られる。
【００７４】図９に、図３のものと同様のフォーマットで、依存関係マスク（「ヒットカウント」）を有するルールを示す。以下のような特殊な記号が、いくつかのホスト名にある。（ｉ）「ドット」記号（．）は、対応するカテゴリのパケットデータを含めることを要求し、（ｉｉ）キャレット記号（＾）は、代わりに異なるカテゴリからのパケットデータを含めることを要求する。「ヒットカウント」は、指定されたアクションがとられるためにキャッシュ内に見つからなければならない一致の数を示す。例えば、「ＲＥＡＬＡＵＤＩＯ」という名前の依存関係マスクでは、１個の必須のＴＣＰセッションがアクティブである限り、ＵＤＰパケットを通過させるためにはカウント１が用いられる。依存関係マスク「ＴＥＬＮＥＴ」では、リソースの過負荷を防ぐためにパケットを廃棄するように、カウント１０が用いられる。
【００７５】図１０に依存関係マスク処理を例示する。これは以下のステップを含む。
【００７６】９０１：パケットを取得し、セッションキーを抽出する。
【００７７】９０２：プロセスはルールセットエントリを順に処理する。与えられたルールで一致が見つからない場合、プロセスはセット内の次のルールに進む。ルールセットの終端まで一致が見つからない場合、パケットは廃棄される。一致が見つかり、依存関係マスクフィールドが空の場合、プロセスはステップ９０５に飛ぶ。
【００７８】９０３：パケットおよびインタフェース情報が、キャッシュ探索構造体（例えば、問合せ）の形成に含められる。依存関係マスクにおいてユーザ認証フラグがセットされている場合、キャッシュ探索構造体における対応するフラグがセットされる。このステップは、ルールの問合せ部分を定義している。
【００７９】９０４：キャッシュで、キャッシュ探索構造体と一致するものを探索し、一致のカウントを積算する。このステップは、ルールの問合せ部分を処理している。
【００８０】９０５：積算カウントがヒットカウント以上である場合、ルールは選択され、そのルールに対応するアクションが実行される。このようなアクションは、通過、廃棄あるいはプロキシを含むことが可能である。また、対応するエントリがキャッシュに作られる。キャ

ッシュにおいて一致が見つからない場合、または、キャッシュに見つかったエントリが「ヒットカウント」より少ない場合、プロセスはステップ９０２に戻り、次のルールに進む。このステップは、問合せの結果に基づいてルールのアクション部分を処理している。

【００８１】上記の依存関係マスク処理を含むルール処理は、ネットワークセッションの最初のパケットに対してのみ実行される。他のすべてのパケットのアクションは、最初のパケットの処理後にセッションキャッシュに保存されているので、他のすべてのパケットは、このルール探索機能を迂回する。

【００８２】４．動的ルール

動的ルールは、例えばルール処理エンジンによって、アクセスルールとともに処理するために、必要が生ずるのに応じてアクセスルールとともに含められるルールである。動的ルールは、例えば、特定のソースおよびデスティネーションのポート番号のような、固有の現在の情報を含むことが可能である。動的ルールは、信頼されたパーティ、例えば、信頼されたアプリケーション、リモートプロキシあるいはファイアウォールアドミニストレータによって、特定のネットワークセッションに権限を与えるためにいつでもロードされることが可能である。動的ルールは、単一セッション用に設定されることも可能であり、あるいは、その使用は期限付きとすることも可能である。動的ルールによれば、ルールセット全体をリロードすることを要求することなく、与えられたルールセットを、ネットワークで起こるイベントに基づいて修正することが可能となる。

【００８３】動的ルールの例としては、単一のセッションに対してのみ用いられる「ワンタイム」ルール、指定された期間に対してのみ用いられる時限ルール、および、ある条件が満たされたときにのみ用いられるしきい値ルールがある。他のタイプの動的ルールとしては、ホストグループを定義するルールがある。この動的ルールによれば、アクセスルールセットの他の事項を変更せずに、ホストを追加あるいは削除するようにホストグループを変更することができる。他の動的ルールとしては、ある特定のタイプの処理アプリケーションにおけるルールセットアップを容易にするために用いられるものがある。例えば、ＦＴＰプロキシアプリケーションは、動的ルールを用いて、データ要求に応じてＦＴＰデータチャネルの確立の権限を与えることが可能である。この例における動的ルールは、一般に、ＦＴＰ制御セッションを通じてデータ要求がなされるまではロードされず、また、１回の使用に限定され、制限された期間の間のみアクティブとされる。従って、ルールセットは、すべての要求とともに用いられる別個のデータチャネルルールを含む必要がない。その結果、ルール仕様およびルール処理が単純化されるとともに、セキュリティが改善される。

【００８４】５．プロキシ反射

本発明によるプロキシ反射とは、ネットワークセッションを、処理のために他の「リモート」プロキシサーバにリダイレクトした後、ファイアウォールを通じて目的のデスティネーションへ渡すものである。新しいセッションがファイアウォールに入ると、プロキシサーバによるサービスが要求されているかどうかが判定される。プロキシサーバによるサービスが要求されている場合、ファイアウォールは、パケット内のデスティネーションアドレスを、プロキシアプリケーションのホストアドレスで置き換える。必要であれば、ファイアウォールは、サービスポートも変更することが可能である。プロキシアプリケーションは、そのセッションを受け取ると、デスティネーションへのコネクションの権限が与えられているかどうかを判定するために、ファイアウォールに対して、そのセッションのもとのデスティネーションアドレスを要求する。その後、プロキシが、自己のＩＰアドレスを用いてそのデスディネーションへのコネクションを形成する場合、ファイアウォールによって提供されるサービスを「単一反射」あるいは「一方向反射」という。

【００８５】ユーザおよびプロキシアプリケーションによっては、デスティネーションにおいてコネクションがリモートシステムではなくもとのソースから来ているように見えなければならない場合がある。これは、例えば、ソースＩＰアドレスを検査して、要求されたサービスに対してサインアップしたユーザに一致するかどうかを確認するサービスの場合に当てはまる。この能力は、「二重反射」（あるいは「双方向反射」）によって提供される。この場合、出コネクションのソースアドレスはリモートプロキシからもとのユーザのソースアドレスに変更される（戻される）。この変更は、各パケットがプロキシから受信されてデスティネーションへ送られるときに、ファイアウォールで行われる。

【００８６】二重反射能力を提供するため、プロキシアプリケーションは、ファイアウォールに対して、もとの入ネットワークセッションの詳細を要求する。ファイアウォールは、出コネクションで用いるポート番号を返す。このポート番号は固有のものであり、これによりファイアウォールは、ソースアドレスを正しいユーザソースアドレスにマッピングすることができるように、正しい出コネクションを識別することができる。その結果、プロキシアプリケーションは両方のパーティには見えない。

【００８７】プロキシ反射を実現する際に、図１１および図１２を参照して以下で説明する実施例のように、動的ルールを用いることが可能である。

【００８８】図１１に、プロキシ反射処理を例示する。これは、ファイアウォールにおける以下のステップを含む。

【００８９】１００１：パケットがファイアウォールに

よって受信される。

【0090】1002：適当なセッションキャッシュを調べることによって、あるいは、キャッシュ内に見つからなければ、適当なルールセットを調べることによって、パケットに関係づけられたアクションが判定される。アクションが「通過」または「プロキシ」である場合、パケット処理は継続される。アクションが「廃棄」である場合、パケットは廃棄される。

【0091】1003：アクションが、ファイアウォール上でローカルにサポートされるプロキシアプリケーションを示している場合、パケットは、プロトコルスタックを通じて、待機中のプロキシアプリケーションへ送られる。

【0092】1004：アクションがリモートプロキシを示している場合、パケットのデスティネーションアドレスがリモートプロキシのアドレスで置き換えられる。設定により、デスティネーションポートを変更することも可能である。もとのパケットヘッダデータが、変更された値とともにセッションキャッシュに記録される。

【0093】1005：パケットはリモートプロキシサーバへ転送される。

【0094】図12に、リモートプロキシにおける、ステップ1005に続く処理を例示する。これは以下のステップを含む。

【0095】1006：パケットはリモートプロキシサーバアプリケーションで受信される。

【0096】1007：リモートプロキシは、ファイアウォールに対して、パケットのもとのセッションキーを要求する。

【0097】1008：リモートプロキシアプリケーションは、もとのセッションキーを用いて自己の機能（例えば、自己のセキュリティモデルに基づいてコネクションを廃棄する、要求されたサービスを実行する、あるいは、ユーザに代わってもとのデスティネーションアドレスと通信する）を実行する。リモートプロキシが単一反射を用いている場合、プロセスはステップ1011に飛ぶ。

【0098】1009：リモートプロキシアプリケーションは、暗号化されたチャネルを通じて、ファイアウォールに対して二重反射能力を要求する。

【0099】1010：ファイアウォールは、サーバからのコネクションの固有性を保証する新しいデスティネーションポート番号を決定する。ファイアウォールはこの新しいポート番号およびもとのセッションキーをプロキシアプリケーションに返す。

【0100】1011：リモートプロキシアプリケーションは、ファイアウォールに対して、自己からもとのデスティネーションへのコネクションに対する許可を要求する。

【0101】1012：ファイアウォールは、動的ルールをロードしてこのアクションを実行する。

【0102】1013：リモートプロキシは、パケットをファイアウォールに送る。ステップ1012でロードされた動的ルールに基づいて、ファイアウォールはパケットをもとのデスティネーションへ転送する。二重反射の場合、プロキシは、ステップ1010でファイアウォールによって決定されたデスティネーションポートを使用し、パケットがファイアウォール通過するときに、IPヘッダ値はもとの値に戻される。

【0103】同じセッションに関係づけられた後続のすべてのパケットは、ステップ1007および1009～1012を飛ばすことが可能であることを除いては、同様に処理される。これは、セッションが生きている間、同じ動的ルールが適用されるからである。

【0104】本発明は、広範囲のアプリケーションで実施することができる。例えば、本発明は、ダイヤルアップアクセスゲートウェイにおけるファイアウォール性能を改善するために使用可能である。本発明の別の実施例では、ファイアウォールの第1部分がネットワークに存在し、ファイアウォールの第2部分がセットトップボックス、コンピュータあるいはその他の、家庭または会社にあるユーザ端末にあるというように分散的にも実装可能である。後者の実施例によれば、本発明のファイアウォール技術は、例えば、家庭においてインターネットとビデオアクセスの親による制御を提供することが可能である。

【0105】

【発明の効果】以上述べたごとく、本発明によれば、複数のセキュリティドメインをサポートする能力により、単一のファイアウォールが、それぞれ別々のセキュリティポリシーを有する複数のユーザをサポートすることが可能となる。また、相異なるセキュリティポリシーをサブサイト間の通信に適用することができるため、このような能力は、サイト内でも使用可能である。

【図面の簡単な説明】

【図1】ユーザサイトに対するファイアウォール保護を提供するローカルエリアネットワークを通じてインターネットに接続されたいくつかのユーザサイトあるいはドメインの図である。

【図2】インターネットに接続され内部ファイアウォールを有するユーザサイトの図である。

【図3】ルールテーブルを例示する図である。

【図4】キャッシュを例示する図である。

【図5】複数のドメインに対するファイアウォール処理の全体流れ図である。

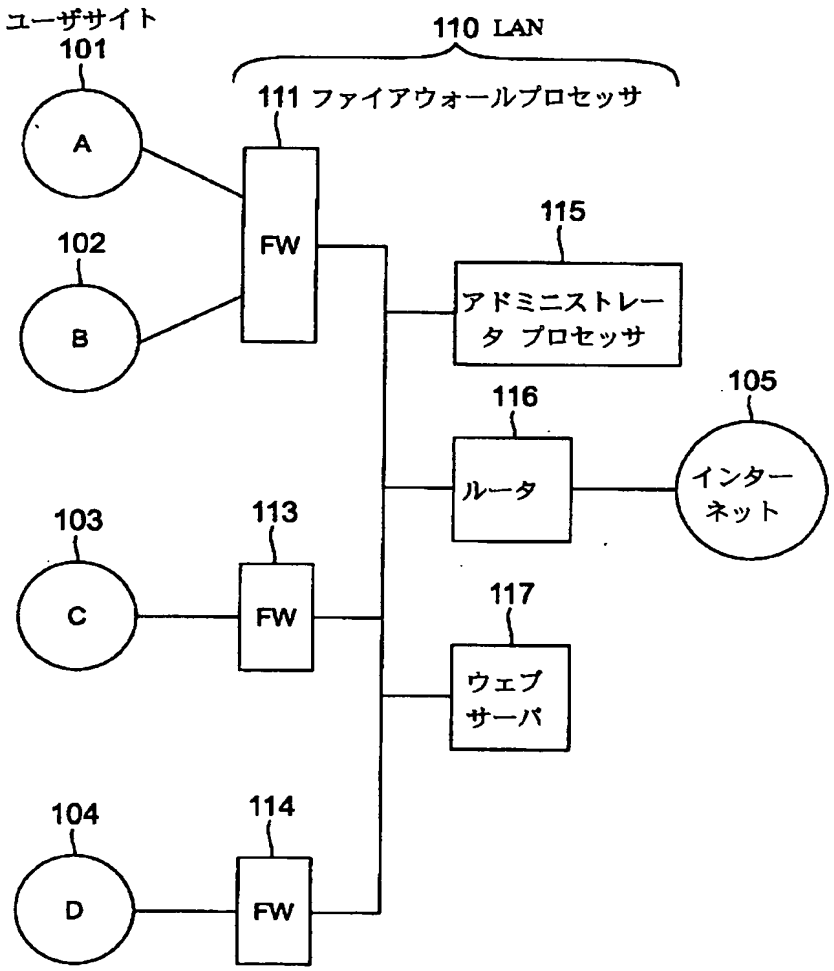
【図6】複数のドメインに対するファイアウォール処理の全体流れ図である。

【図7】ドメインテーブルを例示する図である。

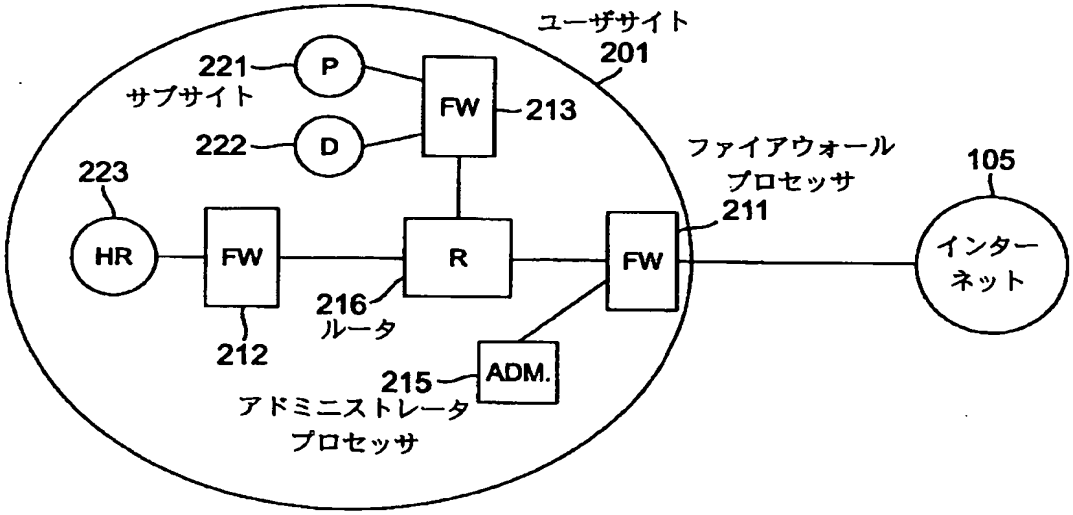
【図8】複数のドメインに対するファイアウォール処理の一部の流れ図である。

【図９】依存関係マスクを例示する図である。
【図１０】依存関係マスク処理の流れ図である。
【図１１】ファイアウォールにおけるプロキシ反射処理の流れ図である。
【図１２】リモートプロキシにおけるプロキシ反射処理の流れ図である。
【符号の説明】
１０１　ユーザサイト
１０２　ユーザサイト
１０３　ユーザサイト
１０４　ユーザサイト
１０５　インターネット
１１０　ＬＡＮ
１１１　ファイアウォールプロセッサ
１１３　ファイアウォールプロセッサ
１１４　ファイアウォールプロセッサ
１１５　アドミニストレータプロセッサ
１１６　ルータ
１１７　ウェブサーバ
２０１　ユーザサイト
２１１　ファイアウォールプロセッサ
２１２　ファイアウォールプロセッサ
２１３　ファイアウォールプロセッサ
２１５　アドミニストレータプロセッサ
２１６　ルータ
２２１　サブサイト
２２２　サブサイト
２２３　サブサイト

【図１】



【図2】



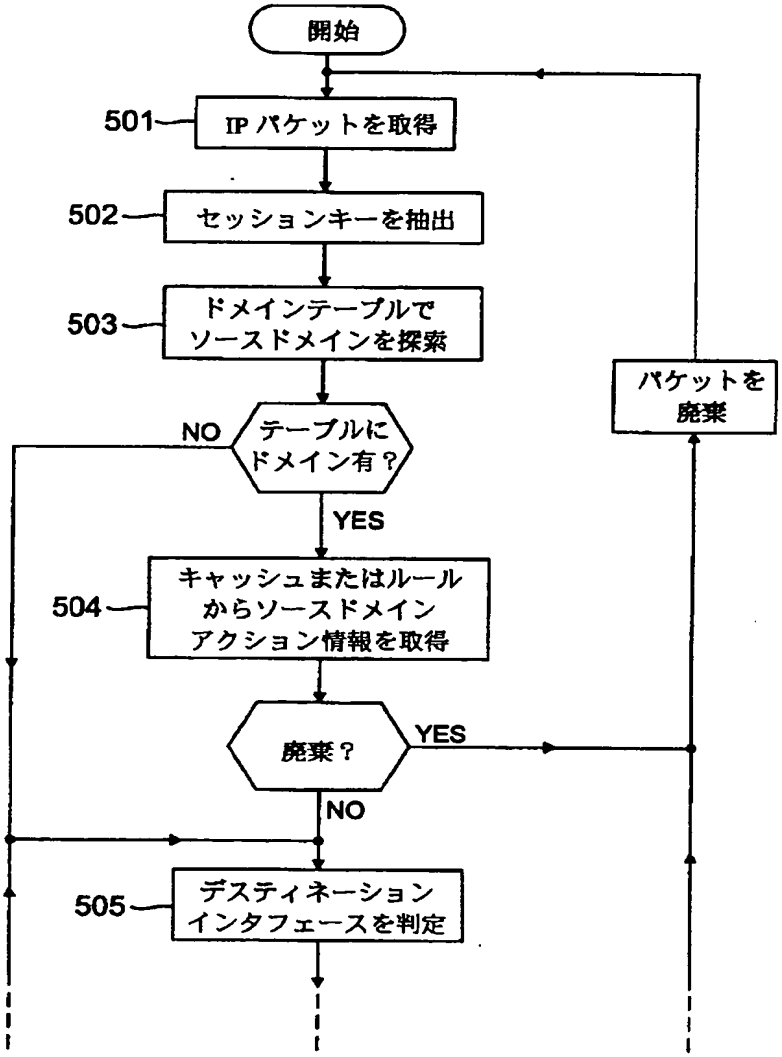
【図3】

ルール番号	ソースホスト	デスティネーションホスト	サービス	アクション
10	A	B	FTP	通過
20	A	*	*	廃棄
30	B	C	TELNET	プロキシ
40	*	D	MAIL	通過

【図4】

セッションキー	ハードウェアアドレス	インタフェース	ルール番号	アラームコード	統計情報	アクション
A, B, TELNET	Ma, Mb	en0, en1	10	10	5パケット	通過
B, A, TELNET	Mb, Ma	en1, en0	10	10	5パケット	通過
C, A, MAIL	Mc, Ma	en1, en0	30	20	100パケット	通過
A, C, MAIL	Ma, Mc	en0, en1	30	20	10パケット	通過
D, A, TELNET	Md, Ma	en1, en0	40	30	15パケット	廃棄
E, A, MAIL	Me, Ma	en1, en0	30	10	30パケット	通過
A, E, MAIL	Ma, Me	en0, en1	30	10	10パケット	通過

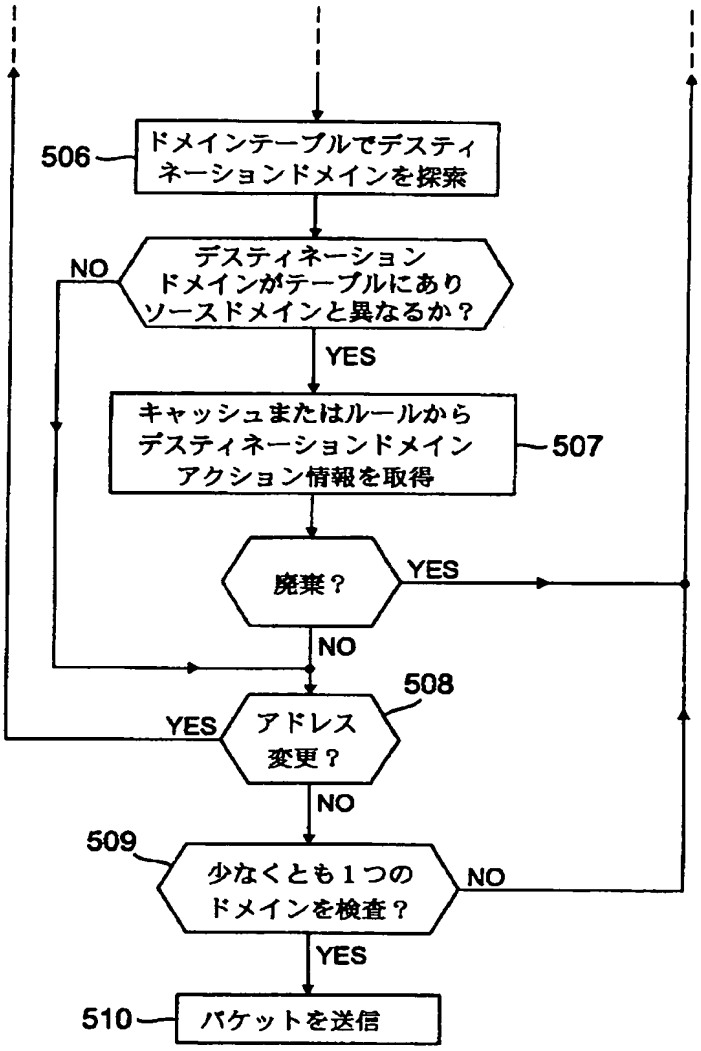
【図5】



【図7】

インタフェース	アドレスレンジ	ドメイン
0	10.50.0.0 – 10.50.255.255	A
0	10.60.0.0 – 10.60.255.255	B
1	*	C
2	*	*

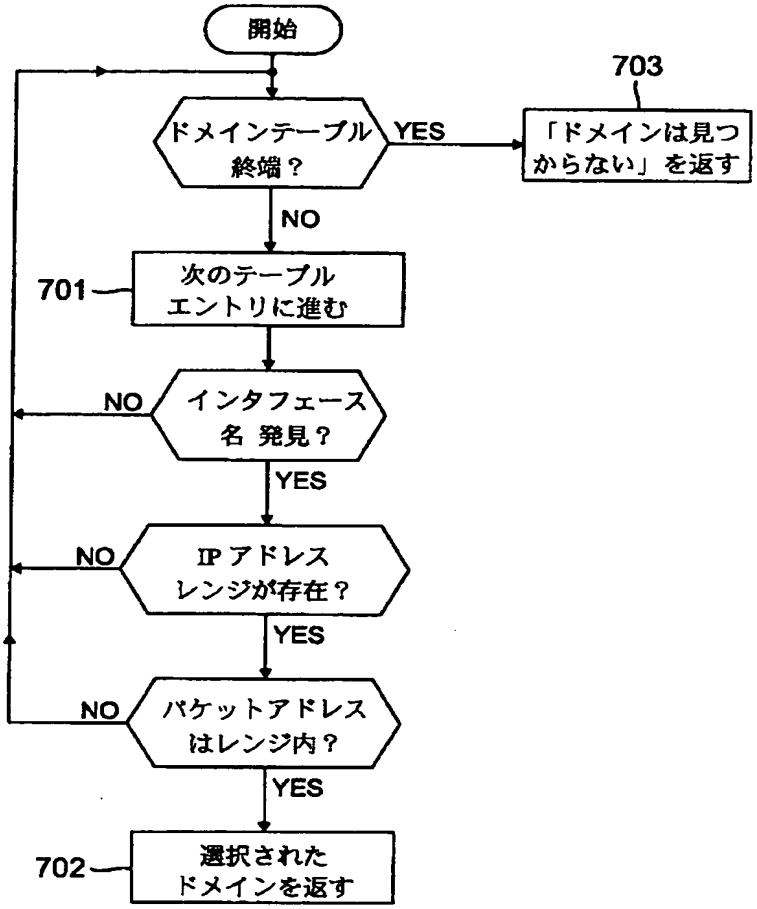
【図6】



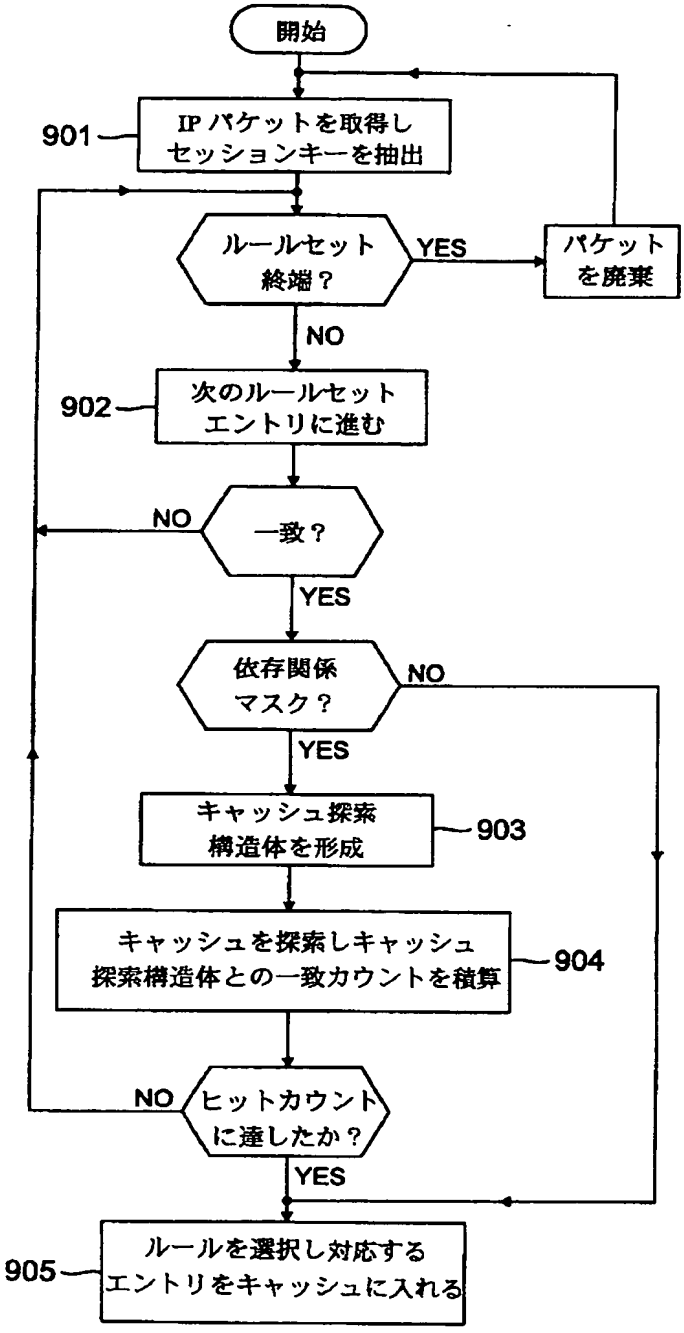
【図9】

名称	ソースホスト	デスティネーションホスト	サービス	アクション	ヒットカウント
TRACEROUTE	*	*	TRACEROUTE	通過	1
PPTP	.	.	TCP/1723	通過	1
TELNET	A	B	TELNET	廃棄	10
REALAUDIO	*	*	TCP/7070	通過	1

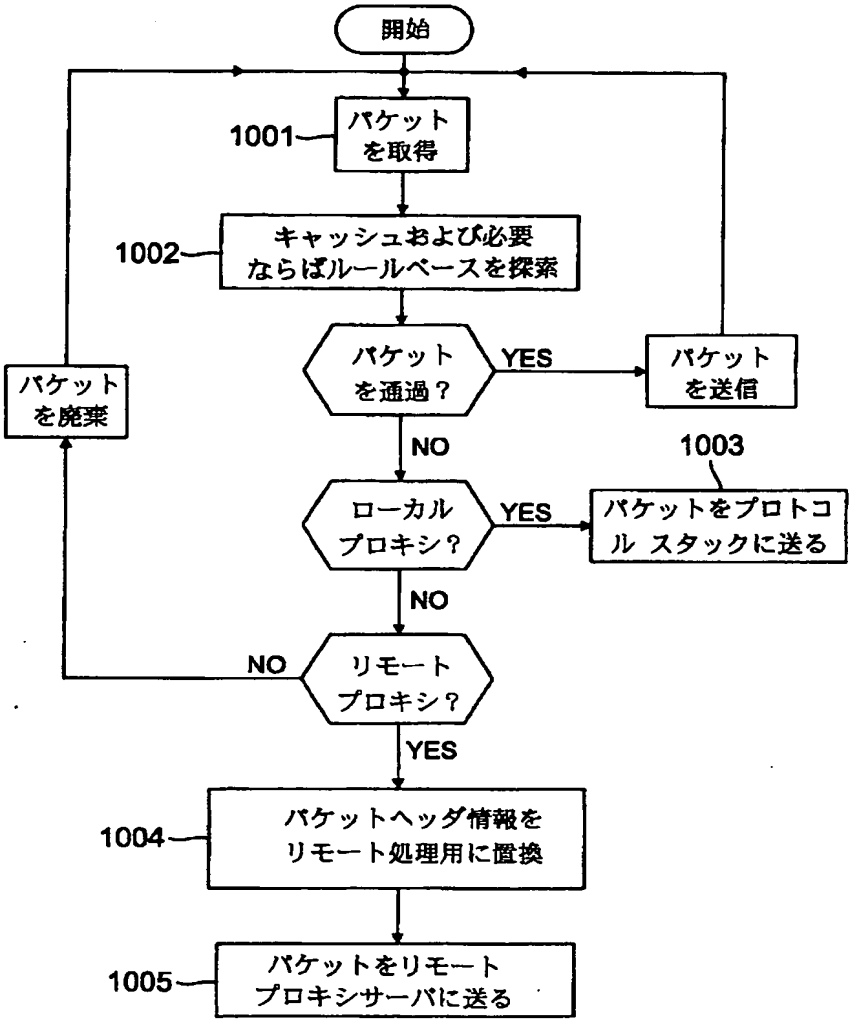
【図8】


開始
ドメインテーブル終端？
YES
703
「ドメインは見つからない」を返す
NO
701
次のテーブルエントリに進む
NO
インタフェース名 発見？
YES
NO
IPアドレスレンジが存在？
YES
NO
パケットアドレスはレンジ内？
YES
702
選択されたドメインを返す

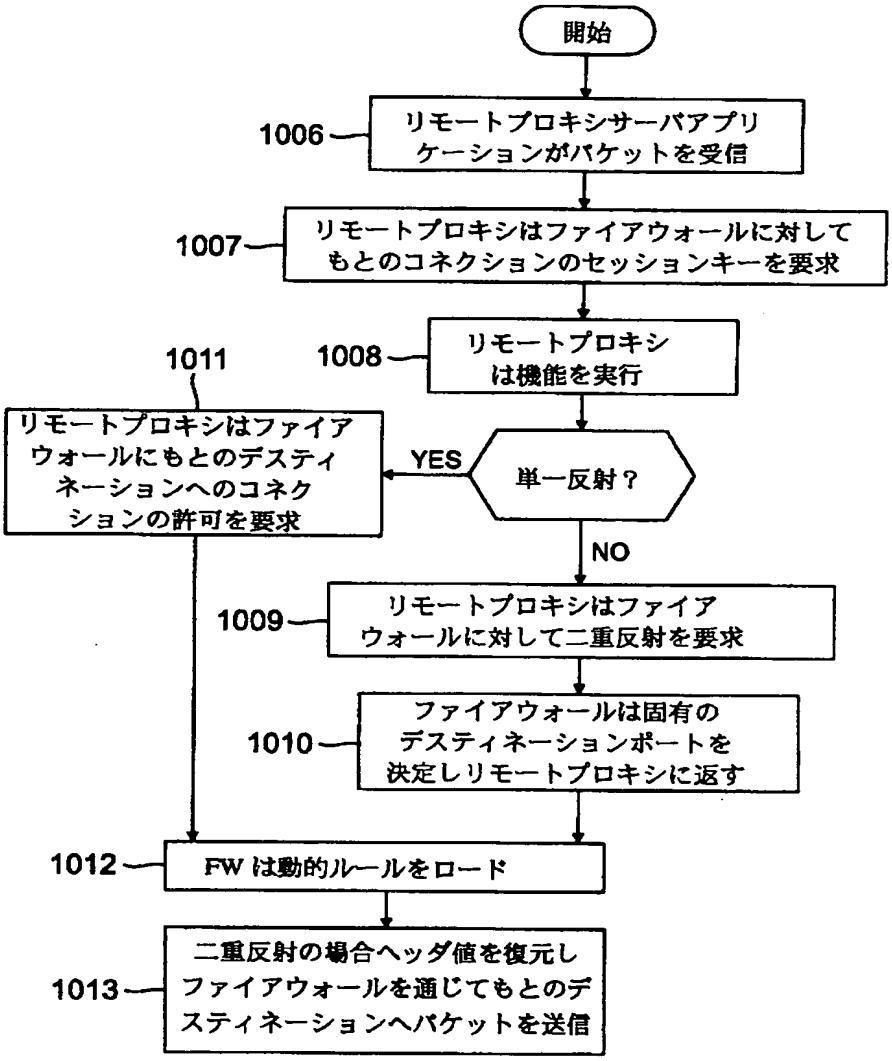
【図10】


開始
IPパケットを取得し
セッションキーを抽出
901
ルールセット
終端？
YES
パケット
を廃棄
NO
次のルールセット
エントリに進む
902
NO
一致？
YES
依存関係
マスク？
NO
YES
キャッシュ探索
構造体を形成
903
キャッシュを探索しキャッシュ
探索構造体との一致カウントを積算
904
NO
ヒットカウント
に達したか？
YES
ルールを選択し対応する
エントリをキャッシュに入れる
905

【図11】


開始
1001
パケットを取得
1002
キャッシュおよび必要ならばルールベースを探索
パケットを通過？
YES
パケットを送信
パケットを廃棄
NO
1003
ローカルプロキシ？
YES
パケットをプロトコル スタックに送る
NO
NO
リモートプロキシ？
YES
1004
パケットヘッダ情報をリモート処理用に置換
1005
パケットをリモートプロキシサーバに送る

【図12】



フロントページの続き

(71)出願人　596077259
600 Mountain Avenue, Murray Hill, New Jersey 07974-0636U. S. A.

(72)発明者　デヴィッド　エル．マジェット
アメリカ合衆国，07924　ニュージャージー，バーナーズヴィル，マレンズ　レイン　73

(72)発明者　ロナルド　エル．シャープ
アメリカ合衆国，07830　ニュージャージー，キャリフォン，ギャリー　レイン，レイルロード2　ボックス　245